Самба как контроллер домена без использования LDAP

Автор: lissyara.
Оригинал: http://www.lissyara.su/articles/freebsd/programms/samba_as_pdc_without_ldap/

Это - обновление старой одноимённой статьи. Как и старая - эта полностью копи-пастная - всё работает "из коробки" =) Причина обновления - недоработки старой статьи, кривости в некоторых местах (дополнительные параметры пользователя не редактировались). Ну и столкнулся с практической реализаций решения - попросили сделать в одной конторе.
Задача - поднять домен с целью централизованного хранения учётных записей пользователей, выполнения каких-то скриптов при логине и т.п. Больше оно и не может - ибо уровень домена - NT4.

Система - FreeBSD 7.2-STABLE. Ставим самбу:server$ cd /usr/ports/net/samba3
server$ make install clean

В вылезшем окошке выбираем следующие опции:[X] WINBIND With WinBIND support
[X] ACL_SUPPORT With ACL support
[X] SYSLOG With Syslog support
[X] QUOTAS With Disk quota support
[X] UTMP With UTMP accounting support
[X] POPT With system-wide POPT library
[X] PCH With precompiled headers optimization

Рисуем конфиг /usr/local/etc/smb.conf:#
[global]
workgroup = SRO
netbios name = SERVER
server string = SAMBA Domain Controller For SRO

Скрипт добавления пользователя
add user script = /usr/local/etc/samba/add_user_script.sh "%u"
Скрипт удаления пользователя
delete user script = /usr/sbin/pw userdel "%u" -r
Скрипт переименованя пользователя
(следующие две строки - на самом деле одна. невлезает ..)
rename user script =
/usr/local/etc/samba/rename_user_script.sh "%uold" "%unew"
Скрипт перезапуска самбы (Вообще, в man smb.conf, предлагается

```
# ребутить или класть всю машину. Перебор, по моему... Хотя -
# у меня это не работает. Такчто - пофиг.)
shutdown script = /usr/local/etc/samba/shutdown_script.sh
# Скрипт добавления новой группы
add group script = /usr/sbin/pw groupadd "%g"
# Скрипт удаления группы
delete group script = /usr/sbin/pw groupdel "%g"
# Скрипт добавления пользователя в группу
# (следующие две строки - это одна, в ширину сайта на вписывается)
add user to group script =
/usr/local/etc/samba/add_user_to_group_script.sh "%g" "%u"
# Скрипт установки первичной группы для пользователя
set primary group script = /usr/sbin/pw usermod "%u" -g "%g"
# Скрипт удаления пользователя из группы
# (следующие две строки - это одна, в ширину сайта на вписывается)
delete user from group script =
/usr/local/etc/samba/delete_user_from_group_script.sh "%g" "%u"
# Скрпит для добавления аккаунта компьютера
add machine script = /usr/local/etc/samba/add_machine_script.sh "%u"
# Скрипт проверки пароля (чтобы не пихали 12345 и прочее. Должен вернуть 0
# если пароль нормальный, и что-то другое - если нет. Пароль передаётся
# на стандартный ввод скрпита)
check password script = /path/to/password/check/script.sh
# Скрпит - чё елать при получении сообщений по winpopup (из man`a)
message command = /bin/mail -s 'message from %f on %m' root < %s; rm %s

# added by lissyara 2009-09-04 in 08:50
passdb backend = tdbsam:/usr/local/etc/samba/passdb.tdb
# added by lissyara 2009-09-04 in 09:36
display charset         = koi8-r
unix charset            = koi8-r
dos charset             = koi8-r


# Где лежат скрпиты, выполняемые доменными компами при загрузке
#logon script = scriptslogon.bat
logon script = net_map.bat
domain logons = Yes
os level = 85
preferred master = Yes
domain master = Yes
idmap uid = 5000-9999
idmap gid = 5000-9999

# Кого не пускать
# в итоге она у меня раскомментирована, но настройку
```

```
 # я делал с закомменченой.
 # настоятельно рекомендую расккомментить, после настройки и введения
 # самой машины в домен
 #invalid users = root


 #interfaces = 192.168.120.253/24
 security = user
 # Включаем поддержку WINS
 wins support = yes
 # Указываем виндовый WINS из другого домена - на время, пока он ещё жив
#       wins server = 192.168.0.251
 dns proxy = yes
 time server = True

 # Перемещаемые профили (если не указать эти пункты пустыми -
 # профили у пользователей будут перемещаемые)
#        logon path = \lissyaraprofiles%U
 logon path =
 logon home =
 template homedir =

 # логгинг
#        log level = 10 passdb:10 auth:10 winbind:10
#       log level = 6
 log file = /var/log/samba/log.%m

 # added by lissyara 2009-09-04 in 16:22 MSK
 admin users     = "@SRODomain Admins"


[IPC$]
 path = /tmp


[print$]
 comment = Printer Drivers Share
 path = /usr/home/samba/drivers

[netlogon]
 path = /nethome/samba/netlogon
 read only = no
 browseable = yes

[profiles]
 path = /nethome/samba/profiles
```

```
 browseable = yes
 create mask = 0600
 directory mask = 0700
 read only = no
 guest ok = yes
```

Набор шар - опционален, обязательны лишь первые три. Далее - рисуем описанные в конфиге скрипты по управлению пользователями и группами, но, не забываем добавить в /etc/rc.conf такую строку:samba_enable="YES"

Скрипт добавления пользователя для компьютера добавляемого в домен - add_machine_script.sh:#!/bin/sh

```
# скрипт добавления машины
/usr/sbin/pw useradd "$1" -d /dev/null
 -s /sbin/nologin -L "russian" -m
 -g computers -c "computer_account"

# отладка
echo "added komp '$@' in `date +%Y-%m-%d` `date +%H:%M:%S`"
 >> /tmp/`basename $0`.log
```

Скрипт добавления пользователя - add_user_script.sh:#!/bin/sh

```
# скрипт добавления пользователей
#/usr/sbin/pw useradd "$1" -d /usr/home/samba/profiles/"$1"
#       -s /sbin/nologin -L "russian" -m -g ntusers -c "$1"
/usr/sbin/pw useradd "$1" -d /dev/null
 -s /sbin/nologin -L "russian" -m -g ntusers -c "$1"
# отладка
echo "added user '$@' in `date +%Y-%m-%d` `date +%H:%M:%S`"
 >> /tmp/`basename $0`.log
```

Добавление пользователя в группу - add_user_to_group_script.sh:#!/bin/sh

```
/usr/sbin/pw groupmod "$1" -m "$2"

# отладка
echo "added user '$2' to group '$1' ($@) in `date +%Y-%m-%d`
 `date +%H:%M:%S`" >> /tmp/`basename $0`.log
```

Скрипт для удаления пользователя из группы - delete_user_from_group_script.sh:#!/bin/sh

```
/usr/sbin/pw groupmod $1 -d $2


echo "deleted user '$2' from group '$1' ($@) in `date +%Y-%m-%d`
 `date +%H:%M:%S`" >> /tmp/`basename $0`.log
```

Скрипт переименовывания пользователя - rename_user_script.sh:#!/bin/sh

```
/usr/sbin/pw usermod $1 -l $2

echo "renamed user '$1' --> '$2' ($@) in `date +%Y-%m-%d`
 `date +%H:%M:%S`" >> /tmp/`basename $0`.log
```

Скрипт перезапуска сервиса - shutdown_script.sh:#!/bin/sh

```
# Перезапукаем самбу (в бакгроунде - обязательно!)
/usr/local/etc/rc.d/samba restart &
```

В принципе, все эти скрипты не обязательны. Все они состоят из одной строки, и прекрасно вставляются в конфиг самбы. Вот тока логгировать так проще, при отладке и т.п. Ну и потом по-быстрому глянуть - чё происходило на машине - тоже можно. Так что - ваш выбор - что хотите логгировать - через скрипты, что не хотите - пямо в конфиг команду вписывайте. На мой взгляд - как мимнимум - добавление/удаления пользователей, тоже самое для модификации групп пользователя.

Написанные скрипты делаем исполняемыми и запускаем самбу:server$ chmod +x /usr/local/etc/samba/*.sh
server$ /usr/local/etc/rc.d/samba restart

Заводим пользователя root в самбе (в принципе, опять же, не обязательно - можно дальше действовать от административного пользователя, котрый и будет позднее постоянно использоваться. Но - на этом этапе так будет прощще):server$ smbpasswd -a root
New SMB password:
Retype new SMB password:
Added user root.

Рисуем скрипт добавления нужных системных групп, и маппинга виндовых групп на системные:#!/bin/sh

```
#!/bin/bash
#### Keep this as a shell script for future re-use

pw groupadd ntadmins
pw groupadd ntusers
pw groupadd computers


net groupmap add ntgroup="Domain Admins" unixgroup=ntadmins rid=512 type=d
net groupmap add ntgroup="Domain Users"  unixgroup=ntusers  rid=513 type=d
net groupmap add ntgroup="Domain Guests" unixgroup=nobody rid=514 type=d
net groupmap add ntgroup="Domain Computers" unixgroup=computers type=d
```

Как вы его обзовёте и куда положите - ваше дело. Использоваться он будет лишь один раз. Запускаем:server$ sh samba_group.sh

```
Successfully added group Domain Admins to the mapping db as a domain group
Successfully added group Domain Users to the mapping db as a domain group
Successfully added group Domain Guests to the mapping db as a domain group
No rid or sid specified, choosing a RID
Got RID 3007
Successfully added group Domain Computers to the mapping db as a domain group
```

Добавляем в администраторов будущего домена нужных пользователей (они, разуммется должны уже быть в системе. Я добавляю рута и nik - человек который будет на том конце провода заниматься машинками с виндой):pw groupmod ntadmins -m root

```
pw groupmod ntadmins -m nik
server$ id nik
uid=1001(nik) gid=0(wheel) groups=0(wheel),1982(ntadmins)
server$
```

Зачем рута? Просто все кому делал первым делом пытались залезть на виндовые машины и порулить доменом именно им. (с учётом что я не описываю как заводил того же nik в самбе - так же как и рута - вполне наверно логично...)

Вводим контроллер домена в домен:server$ net join server

```
Password:
Joined domain SRO.
server$
```

Всё. Для верности можно рестартануть самбу и пытаться ввести в домен машины/залогиниться на них юзерами (опять же - если дословно по статье сделано - то только root получиться. ибо в самбе пока больше нет других пользователей).

Оговорки и примечания. В общем - повторяюсь то же что и к предыдущей статье - при удалении пользователя из самбы - грохается системная учётка. Делайте проверку, или юзайте отдельную учётку. При наличии в системе учётки совпадающей по логину с создаваемой - новйо не создаётся - используется существующая.

Сразу отвечаю на впорос - почему не самба 3.3 а 3.0. В 3.3 скрипты, по какой-то причине, выполняются от обычного пользователя, который в винде галки ставит - nik в данном случае. Естессно они не работают. Либо sudo мутить, и ловить остальные глюки, либо - использовать проверенное решение. Я предпочёл последнее.

Для администрирования качаем утилиты http://support.microsoft.com/kb/173673/sr-cs/